Structures algébriques

Extrait du programme officiel :

Le programme, strictement limité au vocabulaire décrit ci-dessous, a pour objectif de permettre une présentation unifiée des exemples usuels. En particulier, l'étude de lois artificielles est exclue.

La notion de sous-groupe figure dans ce chapitre par commodité. Le professeur a la liberté de l'introduire plus tard.

CONTENUS	CAPACITÉS & COMMENTAIRES
a) Lois de composition internes	
Loi de composition interne.	
Associativité, commutativité, élément neutre, inversibilité, distributivité.	Inversibilité et inverse du produit de deux éléments inversibles.
Partie stable.	
b) Structure de groupe	
Groupe.	Notation x^n dans un groupe multiplicatif, nx dans un groupe additif. Exemples usuels : groupes additifs $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, groupes multiplicatifs $\mathbb{Q}^*$, $\mathbb{Q}_+^*$, $\mathbb{R}^*$, $\mathbb{R}_+^*$, $\mathbb{C}^*$, $\mathbb{U}$, $\mathbb{U}_n$.
Groupe des permutations d'un ensemble.	Notation S_X.
Sous-groupe : définition, caractérisation.	
c) Structures d'anneau et de corps	
Anneau, corps.	Tout anneau est unitaire, tout corps est commutatif. Exemples usuels : $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.
Calcul dans un anneau.	Relation $a^n - b^n$ et formule du binôme si a et b commutent.
Groupe des inversibles d'un anneau.	

Table des matières

I LOI DE COMPOSITION INTERNE

1 Définition

Définition : loi de composition interne

Soit E un ensemble non vide.
On appelle **loi de composition interne** sur E toute application

$$\star : \left| \begin{array}{ccc} E \times E & \longrightarrow & E \\ (x,y) & \longmapsto & x \star y \end{array} \right. .$$

Exemples

E1 – Les lois usuelles $+, \times$ sur $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}^n$, $\mathbb{R}^{\mathbb{N}}$, $\mathbb{R}^D$ dont des lois de composition interne.

E2 – Les lois $\cup$, $\cap$, $\setminus$, Δ sur $\mathscr{P}(E)$ sont des lois de composition interne.

E3 – La loi $\circ$ sur E^E est une loi de composition interne.

Définition : associativité, commutativité, distributivité

Une loi de composition interne $\star$ sur un ensemble E est dite

- **associative** lorsque

$$\forall\, (x,y,z) \in E^3,\quad (x \star y) \star z = x \star (y \star z)$$

(que l'on peut alors noter $x \star y \star z$.)

- **commutative** lorsque

$$\forall\, (x,y) \in E^2,\quad x \star y = y \star x.$$

Si $\star$ et $\top$ sont deux lois de composition interne sur E, on dit que $\star$ est **distributive** sur $\top$ lorsque

$$\forall\, (x,y,z) \in E^3,\quad x \star (y \top z) = (x \star y) \top (x \star z) \text{ et } (y \top z) \star x = (y \star x) \top (z \star x).$$

Exemples

E1 – $x \star y = \dfrac{x+y}{2}$ sur $\mathbb{R}$ n'est pas associative. (prendre -1, 0 et 1).

E2 – $\circ$ sur E^E n'est en général ni commutative, ni distributive sur $+$ (elle l'est en fait à droite, mais pas à gauche).

Remarque

- **Notation additive d'une loi associative** (souvent pour des lois commutatives) :

$$\underbrace{x+x+\cdots+x}_{n \text{ fois}} = nx.$$

On vérifie alors sans mal (par récurrence) que

$$\forall\, n,p \in \mathbb{N}^*,\quad (n+p)x = nx+px = px+nx.$$

- **Notation multiplicative d'une loi associative** :

$$\underbrace{x\cdot x\cdot\cdots\cdot x}_{n \text{ fois}} = x^n.$$

On vérifie alors sans mal (par récurrence) que

$$\forall\, n,p \in \mathbb{N}^*,\quad x^{n+p} = x^n\cdot x^p = x^p\cdot x^n.$$

⚠ En général, $(x\cdot y)^n = (x\cdot y)\cdot(x\cdot y)\cdot\cdots\cdot(x\cdot y) \neq x^n\cdot y^n$.

En plus d'être associative, la loi doit être commutative.

2 Élément neutre

Définition : Élément neutre

Soit $\star$ une loi de composition interne sur E et e un élément de E.
On dit que e est **élément neutre** pour $\star$ si pour tout $x \in E$, $x \star e = e \star x = x$.

Propriété : Unicité de l'élément neutre

S'il existe, l'élément neutre est unique.

Démonstration

$e = e \star e' = e'$ car e est neutre à gauche et e' est neutre à droite. □

Remarque

- **Notation additive** : $0x = e$ avec e souvent noté 0 ou 0_E appelé élément nul.
- **Notation multiplicative** : $x^0 = e$ avec e souvent noté 1 ou 1_E appelé élément unité.

Exemple

E et $\varnothing$ pour $\cap, \cup$ sur $\mathscr{P}(E)$, pour $(0)_n$ et $(1)_n$ pour $+, \times$ sur $\mathbb{R}^{\mathbb{N}}$, id_E pour $\circ$ sur E^E.

3 Eléments symétrisable

Définition : Éléments symétrisables

Soit $\star$ une loi de composition interne sur E, admettant un élément neutre $e \in E$.

Un élément x de E est dit **symétrisable** pour $\star$ si on a $y \in E$ tel que $x \star y = y \star x = e$.

Définition - Propriété : Unicité du symétrique

Si $\star$ est une loi de composition interne associative sur E, alors pour tout $x \in E$ symétrisable, l'élément y de E tel que $x \star y = y \star x = e$ est unique et appelé **symétrique** de x pour $\star$ dans E.

Démonstration

Si y, y' conviennent, alors $y' = y' \star (x \star y) = (y' \star x) \star y = y$. □

Remarques

R1 –
- **Notation additive** : on parle d'opposé, noté $-x$. Pour $x + (-y)$, on note $x - y$.
- **Notation multiplicative** : on parle d'inverse, noté x^{-1}.
  ⚠ $\frac{x}{y}$ n'a pas de sens en général : cela désigne $x \star y^{-1}$ ou $y^{-1} \star x$?

R2 – L'élément neutre e (lorsqu'il existe) est toujours symétrisable, de symétrique lui-même, car $e \star e = e$.

R3 – Être symétrisable à gauche ou à droite ne suffit pas.

Exemple

Sur E^E pour $\circ$, l'élément neutre est id_E.
- $\left(\exists g \in E^E \mid f \circ g = g \circ f = \mathrm{id}_E\right) \iff f$ bijective (ie inversible pour $\circ$).
- $\left(\exists g \in E^E \mid f \circ g = \mathrm{id}_E\right) \iff f$ surjective.
- $\left(\exists g \in E^E \mid g \circ f = \mathrm{id}_E\right) \iff f$ injective.

R4 – Vu la démonstration, si on a un symétrique à gauche et un symétrique à droite, ils sont égaux et l'élément est symétrisable.

Exemples

E1 – Sur $\mathscr{P}(E)$ avec $\cap$: seul E est inversible et $\cup$: seul $\varnothing$ est inversible.

E2 – Sur $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$, description des symétrisables pour $+$ et $\times$.

Propriété

Soit $\star$ une loi de composition interne associative sur E.
Si x et y sont symétrisables, alors
- *$x \star y$ l'est aussi. De plus, $\mathrm{sym}(x \star y) = \mathrm{sym}(y) \star \mathrm{sym}(x)$.*
- *$\mathrm{sym}(x)$ l'est aussi et $\mathrm{sym}(\mathrm{sym}(x)) = x$.*

Remarque

Avec des notations multiplicatives, $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$ et $\left(x^{-1}\right)^{-1} = x$.

Démonstration

$(x \star y) \star (\mathrm{sym}(y) \star \mathrm{sym}(x)) = e$ par associativité, et de même $(\mathrm{sym}(y) \star \mathrm{sym}(x)) \star (x \star y) = e$, d'où la conclusion, par unicité du symétrique.
Puis $\mathrm{sym}(x) \star x = x \star \mathrm{sym}(x) = e$. □

Corollaire

- *En notation additive : si x est symétrisable, alors pour tout $n \in \mathbb{N}$, nx l'est aussi et $n(-x) = -(nx)$ noté $(-n)x$.*

- *En notation multiplicative : si x est inversible, alors pour tout $n \in \mathbb{N}$, x^n l'est aussi et $\left(x^{-1}\right)^n = (x^n)^{-1}$ noté x^{-n}.*

Démonstration

Récurrence à partir de la propriété précédente appliquée avec $x = y$. □

Remarque

Cela permet de définir kx (resp. x^k) pour $k \in \mathbb{Z}$ lorsque x est symétrisable dont on montre les propriétés habituelles par récurrence et passage à l'inverse/opposé.

II STRUCTURE DE GROUPE

1 Défintion

Définition : Groupe

On appelle **groupe** tout couple $(G, \star)$ où G est un ensemble tel que
- $\star$ est une loi de composition interne sur G
- $\star$ est associative
- G admet un élément neutre pour $\star$
- Tout élément de G admet un symétrique dans G pour $\star$.

Si, de plus, $\star$ est commutative, on dit que $(G, \star)$ est un **groupe commutatif** ou **groupe abélien**.

Remarque

En particulier, un groupe n'est jamais vide.

Propriété : Exemples de groupes usuels

(i) $(\mathbb{C}, +)$ *et* $\left(\mathbb{C}^D, +\right)$ *avec* D *ensemble non vide ont une structure de groupe additif abélien.*

(ii) $(\mathbb{C}^*, \times)$ *a une structure de groupe multiplicatif abélien.*

(iii) $(\mathfrak{S}(E), \circ)$ *a une structure de groupe, non commutatif en général.*

*Si $E = [\![1, n]\!]$, $\mathfrak{S}(E)$ est note $\mathfrak{S}_n$ appelé **groupe symétrique** d'ordre n.*

Démonstration

On applique directement la définition. □

Exemple

$(\mathbb{C}, \times)$, et $(\mathbb{Z}^*, \times)$ ne sont pas des groupes.

Exercice

Soit $(G, \star)$ un groupe. Montrer que tout élément de G est **régulier**, c'est-à-dire que si $x, a, b \in G$,

$$x \star a = x \star b \Longrightarrow a = b$$

et

$$a \star x = b \star x \Longrightarrow a = b$$

Application : Dans chaque ligne et chaque colonne de la table de $\star$, chaque élément de G apparaît exactement une fois.

Exemples

E1 – $G = \{e, a, b\}$, e neutre. On se rend compte qu'on n'a pas le choix pour remplir la table.

$\star$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

$G = \{e, a, a^2 (= a^{-1})\}$. Il n'y a qu'un seul type de groupe à 3 éléments, et il est nécéssairement abélien. On parle de **groupe cyclique** (engendré par a).

Exemple

$\mathbb{U}_3 = \{1, j, j^2\}$

E2 – Pour les groupes à 4 éléments $G = \{e, a, b, c\}$, on se rend compte qu'à une permutation près des éléments, il n'y a que deux types :

$\overset{\curvearrowleft}{\star}$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

$G = \{e, a, a^2, a^3\}$, groupe abélien. On parle de **groupe cyclique** (engendré par a).

Exemple

$\mathbb{U}_4 = \{1, \mathrm{i}, -1, -\mathrm{i}\}$.

$\overset{\curvearrowleft}{\star}$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Groupe abélien, avec $a^2 = b^2 = c^2 = e$. On parle de **Groupe de Klein**.

Exemples

E1 – Si A, B sont deux points du plan, $G = \{\mathrm{id}, s_1, s_2, s_3\}$ pour la loi $\circ$ avec s_1 symétrie d'axe (AB), s_2 symétrie d'axe la médiatrice de $[\mathrm{AB}]$ et s_3 symétrie de centre le milieu de $[\mathrm{AB}]$.

Il s'agit en fait du **groupe diédral** D_4 des isométries laissant globalement invariant un segment $[\mathrm{AB}]$.

E2 – $\mathbb{U}_2^2 = \{(1,1), (-1,1), (1,-1), (-1,-1)\}$ muni du produit coordonnée à coordonnée.

2 Sous-groupes

a Définition

Définition : Sous-groupe

Soit $(G,\star)$ groupe.
On dit que $(H,\star)$ est un **sous-groupe** de $(G,\star)$ si $H \subset G$ et $(H,\star|_{H^2})$ est un groupe.
On note $(H,\star) < (G,\star)$.

Propriété : Sous-groupes triviaux

Soit $(G,\star)$ groupe.
*$(G,\star)$ et $(\{e_G\},\star)$ sont des sous-groupes de $(G,\star)$ appelés **sous-groupes triviaux**.*

Remarques

R1 – $<$ est une relation d'ordre partiel sur l'ensemble des groupes.

R2 – Pour montrer que $(G,\star)$ est un groupe, on essaye en général de le faire apparaître comme sous-groupe d'un groupe connu. Comment ?

b Caractérisation

Propriété

Soit $(G,\star)$ un groupe. Les propositions suivantes sont équivalentes :

(i) $(H,\star)$ est un sous-groupe de $(G,\star)$

(ii)
$$\begin{cases} H \subset G \\ H \neq \varnothing \quad (e_G \in H) \\ H \text{ est stable par } \star \ : \ \forall x,y \in H, \ \ x \star y \in H \\ H \text{ est stable par inverse } \ : \ \forall x \in H, \ \ \mathrm{sym}(x) \in H \end{cases}$$

(iii) $\begin{cases} H \subset G \\ H \neq \varnothing \quad (e_G \in H) \\ \forall\, x, y \in H, \quad x \star \mathrm{sym}(y) \in H \end{cases}$

Remarque

En notation multiplicative, (iii) devient $\begin{cases} H \subset G,\ H \neq \varnothing \quad (e_G \in H) \\ \forall\, x, y \in H, \quad x \cdot y^{-1} \in H \end{cases}$

En notation additive, (iii) devient $\begin{cases} H \subset G,\ H \neq \varnothing \quad (0_G \in H) \\ \forall\, x, y \in H, \quad x - y \in H \end{cases}$

Démonstration

- $(i) \Longrightarrow (ii)$: si $H < G$, $H \subset G$, $H \neq \varnothing$, H stable par $\star$ (Ici) et tout élément de H est symétrisable dans H, donc a fortiori dans G et par unicité, le symétrique dans H sera également le symétrique dans G : $\mathrm{sym}(x)$ car $e_G = e_H$ car $e_h \star e_H = e_H$ et e_H est régulier dans G. Donc $\mathrm{sym}(x) \in H$.
- $(ii) \Longrightarrow (iii)$ facile.
- $(iii) \Longrightarrow (i)$: si on a (iii), alors $H \subset G$. La loi $\star$ est associative sur G donc a fortiori, elle l'est aussi sur H.
  Comme H est non vide, on a $x \in H$ tel $x \star \mathrm{sym}(x) = e_G \in H$. Alors pour tout $x \in H$, $e_G \star \mathrm{sym}(x) = \mathrm{sym}(x) \in H$. e_G est neutre pour $\star$ sur G donc l'est aussi sur H.
  Le symétrique $\mathrm{sym}(x)$ d'un élément de $x \in H$ dans G est dans H, donc tout élément de H est symétrisable dans H.
  Donc $(H, \star)$ est bien un sous-groupe de $(G, \star)$. □

Remarque

Un sous-groupe d'un groupe abélien est facilement encore commutatif.

Propriété : Exemples de groupes usuels

(i) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{R}^D, +)$ *ont une structure de groupe additif abélien.*

(ii) $(\mathbb{Q}^*, \times)$, $(\mathbb{Q}_+^*, \times)$, $(\mathbb{R}^*, \times)$, $(\mathbb{R}_+^*, \times)$, $(\mathbb{U}, \times)$, $(\mathbb{U}_n, \times)$ *pour* $n \in \mathbb{N}^*$ *ont une structure de groupe multiplicatif abélien.*

Démonstration

(i) Sous-groupes de $(\mathbb{C},+)$ ou $(\mathbb{C}^D,+)$.

(ii) Sous-groupes de $(\mathbb{C}^*,\times)$. □

C Intersection et réunion

Propriété

Soit G un groupe et $(H_i)_{i\in I}$ une famille de sous-groupes de G. Alors $\bigcap_{i\in I} H_i$ est un sous-groupe de G.

Démonstration

- $(H_i)_{i\in I} \subset G$ car $\forall\, i\in I,\ \ H_i \subset G$.
- $(H_i)_{i\in I} \neq \varnothing$ car $\forall\, i\in I,\ \ e_G \in H_i$.
- Si $x,y\in (H_i)_{i\in I}$, alors $\forall\, i\in I,\ \ x\star y^{-1}\in H_i$ donc $x\star y^{-1}\in \bigcap_{i\in I} H_i$. □

Propriété

Soit G un groupe, H,K sont des sous groupes de G, alors

$$H\cup K \text{ sous-groupe de } G \iff H\subset K \text{ ou } K\subset H.$$

Démonstration

- $\Longleftarrow$: ok
- $\Longrightarrow$: Si $H\cup K$ sous- groupe de G et $H\not\subset K$, on va montrer que $K\subset H$.
  On a $h\in H\setminus K$.
  Soit $k\in K$. Alors $k\star h\in H\cup K$ par stabilité de $\star$ sur $H\cup G$.
  Si $k\star h\in K$, alors $h=k^{-1}\star(k\star h)\in K$, ce qui n'est pas possible.
  C'est donc que $k\star h\in H$ et donc $k=(k\star h)\star h^{-1}\in H$.
  Finalement, on a bien $K\subset H$. □

d Sous-groupes de $(\mathbb{Z},+)$

Propriété : Sous-groupes de $(\mathbb{Z},+)$

Les sous-groupes de $(\mathbb{Z},+)$ sont exactement les $a\mathbb{Z}$ pour $a \in \mathbb{N}$. De plus, si $Z \neq \{0\}$, $a = \min(\mathbb{Z} \cap \mathbb{N}^*)$.

3 Morphismes de groupes

a Définition

Définition

Soient $(G,\star)$ et $(G',\bullet)$ deux groupes.
$f : (G,\star) \to (G',\bullet)$ est un **morphisme de groupes** si et seulement si

$$\forall (x,y) \in G^2, \quad f(x \star y) = f(x) \bullet f(y)$$

Définition

Lorsque $(G,\star) = (G',\bullet)$, on parle d'**endomorphisme** de groupes.
Lorsque f est bijective, on parle d'**isomorphisme**.
Lorsqu'il existe un isomorphisme entre G et G', on dit que G et G' sont **isomorphes.**
Lorsque f est bijective et $G = G'$, on parle d'**automorphismes**.

Exemples

E1 – $\ln : (\mathbb{R}_+^*,\times) \to (\mathbb{R},+)$ isomorphisme de groupes.

E2 – $\exp : (\mathbb{R},+) \to (\mathbb{R}_+^*,\times)$ isomorphisme de groupes.

E3 – $\left|\begin{array}{ccc} (\mathbb{R},+) & \longrightarrow & (\mathbb{U},\times) \\ \theta & \longmapsto & e^{i\theta} \end{array}\right.$ morphisme de groupes (non injectif).

Remarque

« Être isomorphe à » est une relation d'équivalence sur les morphismes de groupes : on peut montrer que la composée et la réciproque d'un isomorphisme sont des isomorphismes (exercice...)

Propriété

Si $f : (G, \star) \to (G', \bullet)$ est un morphisme de groupes, alors $f(e_G) = e_{G'}$ et pour tout $x \in G$, $f\left(\text{sym}(x)\right) = \text{sym}(f(x))$.

Remarque

En notation multiplicative : $f\left(x^{-1}\right) = \left(f(x)\right)^{-1}$.
En notation additive : $f(-x) = -f(x)$.
On peut avoir un mix des deux : par exemple, si c'est additif au départ et multiplicatif à l'arrivée, ça devient $f(-x) = (f(x))^{-1}$.

Démonstration

$f(e_G) = f(e_G \star e_G) = f(e_G) \star f(e_G)$ donc comme $f(e_G)$ est inversible, $f(e_G) = e_{G'}$.
$f(x) \bullet f(\text{sym}(x)) = f\left(x \star \text{sym}(x)\right) = f(e_G) = e_{G'}$
et $f(\text{sym}(x)) \star f(x) = f\left(\text{sym}(x) \star x\right) = f(e_G) = e_{G'}$ □

b Noyau

Définition

Soit $f : (G, \star) \to (G', \bullet)$ un morphisme de groupes. On appelle **noyau** de f :

$$\text{Ker}\, f = f^{-1}(\{e_{G'}\}) = \{x \in G \mid f(x) = e_{G'}\}.$$

Ainsi, $x \in \text{Ker}\, f \iff f(x) = e_{G'}$.

Exemple

$$f : \left| \begin{array}{ccc} (\mathbb{R}, +) & \longrightarrow & (\mathbb{U}, \times) \\ \theta & \longmapsto & e^{i\theta} \end{array} \right. : \text{Ker}\, f = 2\pi\mathbb{Z}.$$

Propriété

Soit $f : (G, \star) \to (G', \bullet)$ un morphisme de groupe.
- *f est injectif si et seulement si $\operatorname{Ker} f = \{e_G\}$.*
- *f est surjectif si et seulement si $\operatorname{Im} f = G'$.*

Remarque

Ainsi, f est injective si et seulement si $f(x) = e_{G'} (= f(e_G)) \Longrightarrow x = e_G$!

Démonstration

Déjà connu pour surjectif.
Remarquons qu'on a toujours $e_G \in \operatorname{Ker} f$ car $f(e_G) = e_{G'}$.
Si f est injectif, alors $x \in \operatorname{Ker} f \iff f(x) = e_{G'} = f(e_G) \iff x = e_G$, donc $\operatorname{Ker} f = \{e_G\}$.
Si $\operatorname{Ker} f = \{e_G\}$ et si $f(x) = f(x')$, alors (en notation multiplicative)

$$e'_G = f(x) \bullet \left(f(x')\right)^{-1} = f(x) \bullet f\left(x'^{-1}\right) = f\left(x \star x'^{-1}\right)$$

donc $x \star x'^{-1} \in \operatorname{Ker} f$ donc $x \star x'^{-1} = e_G$ donc $x = x'$. f est bien injectif. □

Exemple

La fonction f de l'exemple précédent est donc non injective car $\operatorname{Ker} f = 2\pi\mathbb{Z} \neq \{0\}$.

Propriété

Soit $f : (G, \star) \to (G', \bullet)$ un morphisme de groupes.
Alors $\operatorname{Ker} f$ est un sous-groupe de G et $\operatorname{Im} f$ est un sous-groupe de G'.

Démonstration

- $\operatorname{Ker} f$ est un sous groupe de G :
  - ⋆ $\operatorname{Ker} f \subset G$
  - ⋆ $\operatorname{Ker} f \neq \varnothing$ car $e_G \in \operatorname{Ker} f$ car $f(e_G) = e_{G'}$.
  - ⋆ Si $x, x' \in \operatorname{Ker} f$, f étant un morphisme de groupes,

$$f\left(x \star x'^{-1}\right) = f(x) \bullet f(x')^{-1} = e_{G'} \bullet e_{G'}^{-1} = e_{G'},$$

    donc $x \star x'^{-1} \in \operatorname{Ker} f$.
- $\operatorname{Im} f$ est un sous groupe de G' :
  - ⋆ $\operatorname{Im} f \subset G'$
  - ⋆ $\operatorname{Im} f \neq \varnothing$.
  - ⋆ Si $y, y' \in \operatorname{Im} f$, on a $x, x' \in G$ tels que $y = f(x)$ et $y' = f(x')$. f étant un mor-

phisme de groupes,

$$y \bullet y'^{-1} = f(x) \bullet f(x')^{-1} = f\left(x \star x'^{-1}\right) \in \operatorname{Im} f. \quad \square$$

Exemples

E1 – $f : \left| \begin{array}{ccc} (\mathbb{R},+) & \longrightarrow & (\mathbb{C}^*,\times) \\ \theta & \longmapsto & \mathrm{e}^{\mathrm{i}\theta} \end{array} \right.$ étant un morphisme de groupes, $\operatorname{Im} f = \mathbb{U}$ est un sous-groupe de $(\mathbb{C}^*,\times)$ et $\operatorname{Ker} f = 2\pi\mathbb{Z}$ est un sous-groupe de $(\mathbb{R},+)$.

E2 – $f : \left| \begin{array}{ccc} (\mathbb{C}^*,\times) & \longrightarrow & (\mathbb{C}^*,\times) \\ z & \longmapsto & z^n \end{array} \right.$ étant un morphisme de groupes, $\operatorname{Ker} f = \mathbb{U}_n$ est un sous-groupe de $(\mathbb{C}^*,\times)$. C'est aussi le noyau de $|\cdot| : \mathbb{R}^* \to \mathbb{R}^*$ et l'image de $k \in \mathbb{Z} \mapsto \mathrm{e}^{\frac{2ik\pi}{n}}$.

III ANNEAUX

1 Définition

Définition

Soit A un ensemble, $+,\times$ deux lois de composition internes sur A. On dit que $(A,+,\times)$ est un **anneau** lorsque

- $(A,+)$ est un groupe abélien. L'élément neutre est noté 0_A.
- $\times$ est associative et distributive sur $+$.
- $\times$ admet un élément neutre appelé unité de A, noté 1_A.

Lorsque, de plus, $\times$ est commutative, on dit que $(A,+,\times)$ est un **anneau commutatif.**

Propriété

$(\mathbb{Z},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$, $(\mathbb{C},+,\times)$, $\left(\mathbb{R}^D,+,\times\right)$, $\left(\mathbb{C}^D,+,\times\right)$ (avec $D \subset \mathbb{R}$) sont des anneaux commutatifs.

Démonstration

De simples vérifiactions. Pour les fonctions, la fonction nulle est la fontion constamment nulle et la fonction unité est la fonction constamment égale à 1. □

Remarques

R1 – En particulier $(\mathbb{C}^{\mathbb{N}}, +, \times)$ et $(\mathbb{R}^{\mathbb{N}}, +, \times)$ ont une structure d'anneau.

R2 – Plus généralement, si $(A, +, \times)$ est un anneau, alors avec les lois habituelles, si $D \neq \varnothing$, $(A^D, +, \times)$ est un anneau.

Exercice

$(\mathscr{P}(E), \Delta, \cap)$ est un anneau commutatif.

Élément neutre pour $\varnothing$: E, élément neutre pour $\cap$: E. Les lois sont commutatives et associatives. $\cap$ est distributive sur Δ :

$$A \cap (B \Delta C) = A \cap (B \setminus C) \cap A \cap (C \setminus B) = (A \cap B) \setminus (A \cap C) \cap (A \cap C) \setminus (A \cap B) = (A \cap B) \Delta (A \cap C)$$

2 Diviseurs de zéro et intégrité

Définition : Diviseur de zéro

Soit $(A, +, \times)$ un anneau. Un éléments $a \in A$ est appelé **diviseur de zéro** si

- $a \neq 0_A$.
- On peut trouver $b \in A$ tel que $b \neq 0_A$ et $a \times b = 0_A$.

Exemple

Quels sont les diviseurs de zéro dans $\mathbb{R}^{\mathbb{N}}$?

Définition : Anneau intègre

Un anneau $(A,+,\times)$ est dit **intègre** si
- A est commutatif,
- $A \neq \{0_A\}$ c'est-à-dire $1_A \neq 0_A$,
- A n'admet aucun diviseur de zéro, c'est-à-dire

$$\forall\, a,b \in A,\quad a\times b = 0_A \Longrightarrow a = 0_A \text{ ou } b = 0_A.$$

Exemple

$\mathbb{R},\mathbb{Z},\mathbb{C},\mathbb{Q}$ sont des anneaux intègres. $\mathbb{R}^{\mathbb{N}}$ et plus généralement $\mathbb{R}^D$ avec D contenant au moins deux éléments ne le sont pas.

3 Règles de calcul dans un anneau

Propriété

Soit $(A,+,\times)$ un anneau.

(i) 0_A *est* ***absorbant*** *:*

$$\forall\, a \in A,\quad a\times 0_A = 0_A \times a = 0_A.$$

(ii) $\forall\, a,b \in A,\quad (-a)\times b = a\times(-b) = -(a\times b).$

(iii) Si $n,p \in \mathbb{Z}$ et $a,b \in A$,

- $n(a\pm b) = na \pm nb$,
- $n(pa) = (np)b$,
- $n(ab) = (na)b = a(nb)$,
- $na = (n1_A)\,a = a(n1_A)$.

Remarque

Si $1_A = 0_A$, alors pour tout $x \in A$, $x = x\times 1_A = 0_A$ donc $A = \{0_A\}$. Par contraposée, si $A \neq \{0_A\}$, alors $1_A \neq 0_A$.

Démonstration

$\times$ étant distributive sur $+$, $a\times(0_A) = a\times(0_A+0_A) = 2\,(a\times 0_A)$ donc $a\times 0_A = 0_A$. De même, $0_A\times a = 0_A$.

Donc $0_A = (a-a)\times b = a\times b + (-a)\times b$ d'où $(-a)\times b = -(a\times b)$ De même à droite.

Les autres propriétés se démontre par récurrence. Idée, si $n,p \geqslant 0$ (sinon, il faut adapter...) :

- $n(a\pm b)=(a\pm b)+(a\pm b)+\cdots+(a\pm b)=na\pm nb$ par associativité et commutativité de $+$,
- $n(px)=px+\cdots+px=(x+\cdots+x)+\cdots+(x+\cdots+x)=(np)x$ par associtativité de $+$,
- $n(xy)=xy+\cdots+xy=(x+\cdots+x)y=(nx)y$ par distributivité de $\times$ sur $+$, de même à droite,
- $(n1_A)\,x=(1_A+\cdots+1_A)\,x=x+\cdots+x=nx$, par distributivité de $\times$ sur $+$, de même à droite. □

Propriété

Soit $(A,+,\times)$ un anneau. Si $a,b\in A$ tels que $a\times b=b\times a$ et $n\in\mathbb{N}$; alors

- ***Formule du binôme de Newton*** : $(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^kb^{n-k}$
- ***Factorisation de*** a^n-b^n :

$$\begin{aligned}a^n-b^n&=(a-b)\left(a^{n-1}+a^{n-2}b+a^{n-3}b^2\ldots+ab^{n-2}+b^{n-1}\right)\\&=(a-b)\sum_{k=0}^{n-1}a^kb^{n-1-k}.\end{aligned}$$

Démonstration

Semblable à la preuve dans $\mathbb{C}$. Question : où se sert-on de la commutation de a et b ?

- **Formule du binôme** :
  - ⋆ **Preuve par dénombrement** :

$$(a+b)^n=\underbrace{(a+b)(a+b)\cdots(a+b)}_{n\text{ fois}}$$

En développant, on obtient des termes de la forme $x_1x_2\cdots x_n$ avec $x_i=a$ ou b. Si on veut k termes a, on $\binom{n}{k}$ choix, et le terme vaut a^kb^{n-k} car a et b commutent.

  - ⋆ **Preuve par récurrence** sur n, c'est simple si $n=0$ ou 1. Si c'est vrai pour $n-1$,

$$\begin{aligned}(a+b)^n=(a+b)(a+b)^{n-1}&=(a+b)\sum_{k=0}^{n-1}\binom{n-1}{k}a^kb^{n-1-k}\\&=\sum_{k=0}^{n-1}\binom{n-1}{k}a^{k+1}b^{n-k-1}+\sum_{k=0}^{n-1}\binom{n-1}{k}a^kb^{n-k}\end{aligned}$$

(associativité, distributivité, a et b commutent, dans la seconde somme)

$$(a+b)^n = \sum_{k=1}^{n}\binom{n-1}{k-1}a^k b^{n-k} + \sum_{k=0}^{n-1}\binom{n-1}{k}a^k b^{n-k}$$

(changement d'indice $k \mapsto k-1$)

$$= \sum_{k=0}^{n}\binom{n-1}{k-1}a^k b^{n-k} + \sum_{k=0}^{n}\binom{n-1}{k}a^k b^{n-k}$$

(les termes ajoutés sont nuls)

$$= \sum_{k=0}^{n}\left(\binom{n-1}{k-1} + \binom{n-1}{k}\right)a^k b^{n-k}$$

(associativité, distributivité,

Donc $(a+b)^n = \sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k}$ d'après la formule de Pascal étendue.

- **Factorisation de $a^n - b^n$:**

$$(a-b)\sum_{k=0}^{n-1} a^k b^{n-1-k} = \sum_{k=0}^{n-1}\left(a^{k+1}b^{n-(k+1)} - a^k b^{n-k}\right)$$

(a et b commutent, associativité, distributivité)

$$= a^n b^0 - a^0 b^n = a^n - b^n$$

(somme télescopique)

□

Remarque

Si a et b ne commutent pas,

$$(a+b)^2 = a^2 + ab + ba + b^2$$
$$(a+b)^3 = a^3 + a^2 b + aba + ba^2 + ab^2 + bab + b^2 a + b^3$$

etc.

4 Groupe des inversibles

Définition

Soit $(A, +, \times)$ un anneau.
$a \in A$ est dit **inversible** si et seulement s'il est symétrisable pour $\times$.
Son symétrique est appelé **inverse** de a, noté a^{-1}.
On note U_A ou $U(A)$ ou $A^\times$ l'ensemble des inversibles de A.

Remarque

On parle parfois d'unités de A, d'où la notation...

Exemples

E1 – $U_{\mathbb{R}} = \mathbb{R}^*$

E2 – $U_{\mathbb{Z}} = \{-1, 1\}$

E3 – $U_{\mathbb{R}^{\mathbb{N}}} = \{\text{suites jamais nulles}\}$

E4 – $U_{\mathbb{R}^D} = \{\text{fonctions jamais nulles}\}$

Propriété : Groupe des inversibles

*Si $(A, +, \times)$, alors $(U_A, \times)$ est un groupe appelé **groupe des inversibles** de A.*

Démonstration

On a déjà l'associativité, l'élément neutre car A est un anneau. Comme de plus, tout élément inversible est lui même inversible et comme le produit de deux éléments inversibles l'est encore, on a bien une structure de groupe. □

5 Sous-anneau

Définition : Sous-anneau

Soit $(A, +, \times)$ un anneau. On dit que $(B, +, \times)$ est un **sous-anneau** de $(A, +, \times)$ lorsque $B \subset A$, $1_A \in B$ et $\left(B, +|_{B^2}, \times|_{B^2}\right)$ est un anneau.

Remarque

Une partie peut avoir une structure d'anneau pour les lois induites sans avoir la même unité (ce n'est pas un sous-anneau au sens de la définition précédente.) C'est le cas trivialement de $\{0_A\}$.

Exemple

Soit, dans l'anneau des matrices 2×2, l'ensemble B des matrices $\left(\begin{smallmatrix} a & 0 \\ 0 & 0 \end{smallmatrix}\right)$ pour $a \in \mathbb{K}$. Alors $(B, +, \times)$ est un anneau d'unité $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \neq I_2$.

Propriété : Caractérisation des sous-anneaux

$(B,+,\times)$ est un sous-anneau de $(A,+,\times)$ si et seulement si

$$\begin{cases} B \subset A \\ (B,+) \text{ est un sous-groupe de } (A,+) \\ B \text{ est stable par } \times \ : \ \forall\, x,y \in B, \ \ x \times y \in B \\ 1_A \in B \end{cases}$$

ou, de manière équivalente,

$$\begin{cases} B \subset A \ ; \ 1_A \in B \\ \forall\, x,y \in B, \ \ x+y \in B, \ -x \in B \ \text{ et } \ x \times y \in B \\ \qquad \text{ou} \quad \forall\, x,y \in B, \ \ x-y \in B \ \text{ et } \ x \times y \in B \end{cases}$$

Démonstration

Même principe que pour les sous-groupes, la présence de 1_A n'étant automatique que si B possède un élément inversible, d'où la nécessité d'imposer $1_A \in B$. □

Exemple

$\mathbb{Z}[\sqrt{2}] = \mathbb{Z} + \sqrt{2}\mathbb{Z}$ est un sous-anneau de $\mathbb{R}$.

6 Morphisme d'anneau

Définition : Morphisme d'anneaux

Soient $(A,+,\times)$ et $(A',\oplus,\otimes)$ deux anneaux.
$f : (A,+,\times) \to (A',\oplus,\otimes)$ est un **morphisme d'anneaux** si et seulement si

(i) $\forall\,(a,b) \in A^2, \ \ f(a+b) = f(a) \oplus f(b)$
(ie $f : (A,+) \to (A',\oplus)$ morphisme de groupes)

(ii) $\forall\,(a,b) \in A^2, \ \ f(a \times b) = f(a) \otimes f(b)$

(iii) $f(1_A) = 1_{A'}$

On parle aussi, d'**endomorphisme**, d'**isomorphisme** et d'**automorphisme** d'anneaux.

Propriété

Si $f : (A, +, \times) \to (A', \oplus, \otimes)$ est un morphisme d'anneaux et si a est inversible dans A, alors $f(a)$ l'est dans A' et $f\left(a^{-1}\right) = \left(f(a)\right)^{-1}$.

Démonstration

$f(a)f\left(a^{-1}\right) = f\left(aa^{-1}\right) = f(1_A) = 1_{A'}$ et de même $f\left(a^{-1}\right)f(A) = 1_{A'}$. □

Remarque

Comme on a en particulier un morphisme de groupes additifs, on peut utiliser les propriétés de ceux-ci :

- $f(0_A) = 0_{A'}$,
- pour tout $a \in A$, $f(-a) = -f(a)$,
- $\operatorname{Ker} f = f^{-1}(\{0_{A'}\}) = \{a \in A \mid f(a) = 0_{A'}\}$,
- f est injective si et seulement si $\operatorname{Ker} f = \{0_A\}$.

Cependant, ⚠ si $\operatorname{Ker} f$ est bien un sous-groupe de $(A, +)$, ce n'est pas un sous-anneau car $1_A \notin \operatorname{Ker} f$ (à moins que $1_{A'} = 0_{A'}$, ce qui revient à avoir $A' = \{0_{A'}\}$!) Comme tous les autres axiomes sont vérifiés, on parle parfois de pseudo-anneau.

IV STRUCTURE DE CORPS

Définition

Soit $\mathbb{K}$ un ensemble, $+, \times$ deux lois de composition internes sur $\mathbb{K}$. On dit que $(\mathbb{K}, +, \times)$ est un **corps** lorsque

- $(\mathbb{K}, +, \times)$ est un anneaux.
- $\mathbb{K} \setminus \{0_{\mathbb{K}}\}$ est non vide et tous ses éléments sont inversibles (c'est-à-dire $\mathbb{K} \neq \{0_{\mathbb{K}}\}$ et $U_{\mathbb{K}} = \mathbb{K}^\times = \mathbb{K} \setminus \{0_{\mathbb{K}}\}$.)

ou, de manière équivalente,

- $(\mathbb{K}, +)$ est un groupe abélien,
- $(\mathbb{K} \setminus \{0_{\mathbb{K}}\}, \times)$ est un groupe,
- $\times$ est distributive sur $+$.

Lorsque, de plus, $\times$ est commutative, on dit que $(\mathbb{K}, +, \times)$ est un **corps commutatif.**

Exemple

$\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$ munis des lois $+$ et $\times$ sont des corps, mais pas $\mathbb{Z}$.

Propriété

Tout corps n'admet aucun diviseur de zéro.
En particulier, tout corps commutatif est intègre.
La réciproque est fausse.

Démonstration

Si $ab = 0_{\mathbb{K}}$ et si $a \neq 0_K$, alors a est inversible et $b = a^{-1}ab = a^{-1}0_{\mathbb{K}} = 0_{\mathbb{K}}$ car $0_{\mathbb{K}}$ est un élément absorbant.

Pour la réciproque, $(\mathbb{Z}, +, \times)$ est un anneau intègre qui n'est pas un corps. □

Exemples

E1 – $(\mathbb{R}^{\mathbb{N}}, +, \times)$ et $(\mathbb{R}^D, +, \times)$ (où D contient au moins deux éléments) ne sont pas des corps : ils ne sont pas intègres.

E2 – Il existe des corps finis. On peut même montrer que tout corps fini est commutatif (théorème de Wedderburn), de cardinal une puissance d'une nombre premier.

- $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$, ensemble des entiers modulo 2, muni des lois + et × :

+	0	1
0	0	1
1	1	0

et

×	0	1
0	0	0
1	0	1

- $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z} = \{0, 3\}$, ensemble des entiers modulo 3, muni des lois + et × :

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

et

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

- $\mathbb{Z}/4\mathbb{Z}$ n'est pas un corps : il a bien une structure d'anneau, mais n'est pas intègre car $2 \times 2 = 0$ [4].

Définition : Sous-corps

Soit $(\mathbb{K}, +, \times)$ un corps. On dit que $(\mathbb{L}, +, \times)$ est un sous-corps de $(\mathbb{K}, +, \times)$ lorsque $\mathbb{L} \subset \mathbb{K}$ et $(\mathbb{L}, +|_{\mathbb{L}^2}, \times|_{\mathbb{L}^2})$ est un corps.

Propriété : Caractérisation des sous-corps

$(\mathbb{L},+,\times)$ *est un sous-corps de* $(\mathbb{K},+,\times)$ *si et seulement si*

$$\begin{cases} \mathbb{L}\subset\mathbb{K} \\ (\mathbb{L},+) \text{ est un sous-groupe de } (\mathbb{K},+) \\ (\mathbb{L}\setminus\{0_{\mathbb{K}}\},\times) \text{ est un sous-groupe de } (\mathbb{K}\setminus\{0_{\mathbb{K}}\},\times) \end{cases}$$

ou, de manière équivalente,

$$\begin{cases} \mathbb{L}\subset\mathbb{K} \\ \mathbb{L}\setminus\{0_{\mathbb{K}}\}\neq\varnothing \quad (1_{\mathbb{K}}\in\mathbb{L}) \\ \forall\, x,y\in\mathbb{L},\quad x-y\in\mathbb{L} \\ \forall\, x,y\in\mathbb{L}\setminus\{0_{\mathbb{K}}\},\quad xy^{-1}\in\mathbb{L} \end{cases}$$

Démonstration

Le sens $\Longrightarrow$ ne pose pas de problème. Pour le sens $\Longleftarrow$, on a bien un sous-anneau dont tous les éléments non nuls sont inversibles car $1_{\mathbb{K}}=xx^{-1}\in\mathbb{L}$. □

Définition : Morphisme de corps

Soient $(\mathbb{K},+,\times)$ et $(\mathbb{K}',\oplus,\otimes)$ deux corps.
$f:(\mathbb{K},+,\times)\to(\mathbb{K}',\oplus,\otimes)$ est un **morphisme de corps** si et seulement s'il s'agit d'un morphisme d'anneaux, c'est-à-dire

(i) $\forall\,(x,y)\in\mathbb{K}^2,\quad f(x+y)=f(x)\oplus f(y)$
(ie $f:(\mathbb{K},+)\to(\mathbb{K}',\oplus)$ morphisme de groupes)

(ii) $\forall\,(x,y)\in\mathbb{K}^2,\quad f(x\times y)=f(x)\otimes f(y)$

(iii) $f(1_{\mathbb{K}})=1_{\mathbb{K}'}$

Remarque

Avec (i) et (ii), $f(1_{\mathbb{K}})=\big(f(1_{\mathbb{K}})\big)^2$ et comme $\mathbb{K}'$ est intègre, $f(1_{\mathbb{K}})$ vaut $1_{\mathbb{K}'}$ ou $0_{\mathbb{K}'}$. S'il vaut $0_{\mathbb{K}'}$ et si (ii) est vérifiée, alors $f\equiv 0_{\mathbb{K}'}$.

Exemples

E1 – $\mathrm{id}_{\mathbb{C}}$, $z \mapsto \overline{z}$ sont des automorphismes (involutifs) du corps $\mathbb{C}$.

E2 – Tout morphisme de corps est injectif, car si $x \neq 0_{\mathbb{K}}$, x est inversible donc $f(x)$ est inversible, donc $f(x) \neq 0_{\mathbb{K}'}$ donc $x \notin \mathrm{Ker}\, f$, donc $\mathrm{Ker}\, f = \{0_{\mathbb{K}}\}$.